



Software Engineering Institute

Report from the First CERT-RMM Users Group Workshop Series

Julia H. Allen
Lisa Young

April 2012

TECHNICAL NOTE
CMU/SEI-2012-TN-008

CERT Program

<http://www.sei.cmu.edu>



Copyright 2012 Carnegie Mellon University.

This material is based upon work funded and supported by the United States Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

This report was prepared for the

Contracting Officer
ESC/CAA
20 Shilling Circle
Building 1305, 3rd Floor
Hanscom AFB, MA 01731-2125

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

® CERT is a registered trademark owned by Carnegie Mellon University.

® Capability Maturity Modeling and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

SM IDEAL is a service mark of Carnegie Mellon University.

* These restrictions do not apply to U.S. government entities.

Table of Contents

Acknowledgments	vii
Abstract	ix
1 Introduction	1
1.1 Purpose	1
1.2 Structure of This Report	1
2 Overview of the RUG Workshop Series and CERT-RMM	2
2.1 Overview of the First CERT-RMM Users Group (RUG) Workshop Series	2
2.2 Overview of CERT-RMM	2
3 Architecture of the First RUG Workshop Series	5
3.1 Background	5
3.2 Advance Preparation	5
4 Workshop 1: Planning	7
4.1 Advance Preparation	7
4.2 Topics	7
4.3 Outcomes	8
4.4 Preparation for Workshop 2	9
5 Workshop 2: Improvement Objective	10
5.1 Advance Preparation	10
5.2 Topics	10
5.3 Outcomes	11
5.4 Preparation for Workshop 3	12
6 Workshop 3: Diagnosis	13
6.1 Advance Preparation	13
6.2 Topics	13
6.3 Outcomes	15
6.4 Preparation for Workshop 4	15
7 Workshop 4: Improvement Progress	16
7.1 Advance Preparation	16
7.2 Topics	16
7.3 Outcomes	19
8 Improvements for Future RUG Workshop Series	20
8.1 Contact Us	20
Appendix: 2012 SEPG North America RUG Panel Slides	21
References	35

List of Figures

Figure 1:	CERT-RMM Context	4
Figure 2:	The SEI IDEAL Model [McFeeley 1996]	9
Figure 3:	CERT-RMM Improvement-Project Lifecycle	11

List of Tables

Table 1:	Preparatory Questions	5
Table 2:	Workshop 1 Topics	7
Table 3:	Workshop 2 Topics	10
Table 4:	Workshop 3 Topics	13
Table 5:	Workshop 4 Topics	16

Acknowledgments

The authors would like to acknowledge and thank the members of the first CERT® Resilience Management Model (RMM) Users Group (RUG), for their active participation, candor, hard work, and contributions to CERT-RMM implementation. We greatly appreciate their willingness to be innovators and early adopters of this workshop series and their substantial improvement suggestions, which will greatly benefit future RUG members.

- Mary Ann Blair, Doug Markiewicz, and Chris Ortyl
Carnegie Mellon University Information Security Office
- Kent Anderson, Margaret Munk, and Ric Robinson
Discover Financial Services
- Lynn Penn and Dorna Witkowski
Lockheed Martin Information Systems & Global Solutions
- Todd Bame, Eric Brown, Greg Crabb, Aubrey Surgers, and Jim Wilson
United States Postal Inspection Service

The authors would like to thank William David, Lockheed Martin Enterprise Business Services, for sharing his organization's experiences in its use of CERT-RMM. We would also like to thank Nader Mehravari, formerly with Lockheed Martin Enterprise Business Services, for attending Workshop 2 and advising RUG development team members.

The authors would like to thank our SEI colleagues who graciously gave their time to inform RUG members of their work as part of our workshop lunch presentations: Anne Connell, Rita Creel, Rich Friedberg, Joji Montelibano, Greg Shannon, and David White.

The authors would like to thank our SEI colleagues, all of whom were instrumental in the conduct and success of this users group workshop: Rick Barbour, Rita Briston, Matt Butkovic, Jim Cebulla, Pamela Curtis, Linda Parker Gates, Lora Gress, Barbara Tyson, David Ulicne, Jeff Welch, David White, and Katie Palermo Worthy.

Last, but certainly not least, the authors would like to thank Rich Caralli for his thought leadership and sponsorship of this users group workshop.

Abstract

This report describes the first CERT[®] Resilience Management Model (RMM) Users Group (RUG) Workshop Series and relays the experiences of participating members and CERT staff. This workshop series comprised four workshops, which took place between March 2011 and February 2012. In this report, we provide a brief overview of the CERT Resilience Management Model (CERT-RMM), describe the architecture for this series of workshops, and present suggestions for improving future RUG Workshop Series.

1 Introduction

1.1 Purpose

The purpose of this report is to describe the first CERT[®] Resilience Management Model (RMM) Users Group (RUG) Workshop Series and relay experiences of members who participated in it and CERT staff who conducted it. The RUG workshop was originally conceived as a means to help CERT Resilience Management Model (CERT-RMM) users progress in their adoption of the model and get practice using it after taking the three-day Introduction to CERT-RMM course. The workshop was also intended to 1) help CERT staff members understand the requirements necessary to implement CERT-RMM and 2) develop materials that would help users put CERT-RMM practices into action on their specific improvement projects.

1.2 Structure of This Report

Section 2 provides a brief overview of first CERT-RMM Users Group Workshop Series and CERT-RMM.

Section 3 provides background about the first RUG Workshop Series and the steps RUG members took during the preparatory phases.

Sections 4–7 outline the preparation, topics, results, and next steps for the four workshops that constituted the first RUG Workshop Series; these workshops were held March 2011, May 2011, August 2011, and January/February 2012.

Section 8 lists suggestions for improving future RUG workshops.

The appendix includes the RUG panel presentation given at the Software Engineering Institute's (SEI's) 2012 Software Engineering Process Group Conference, North America. The presentation includes slides provided by four of the five RUG member organization.

2 Overview of the RUG Workshop Series and CERT-RMM

2.1 Overview of the First CERT-RMM Users Group (RUG) Workshop Series

The purpose of the first RUG Workshop Series is to offer RUG members an opportunity to engage in customized collaborative discussions, hands-on activities, and workshop exercises and assignments that help them to

- implement a solution that meets a specific resilience improvement objective that is tied to an organizational goal
- improve the effectiveness and efficiency of operational risk management activities
- diagnose their current resilience activities against CERT-RMM processes and practices
- conduct peer-to-peer comparisons and learn from others, including CERT-RMM developers and lead appraisers
- define processes and identify measures to evaluate and improve resilience
- learn how to reduce the complexity and improve the efficiency of compliance and other assessment-related activities
- learn more about current CERT work from guest speakers

The RUG Workshop Series comprised four workshops, which took place between March 2011 and February 2012. RUG members were interviewed in advance of the first workshop so that the RUG Development Team (RDT) could better understand their objectives and requirements and use these to shape the RUG Workshop Series.¹ In addition, between workshops, the RDT held periodic conference calls to discuss issues and ongoing preparatory assignments.

Members of the first RUG Workshop Series included the Information Security Office from Carnegie Mellon University (CMU), representing academia; Discover Financial Services (DFS), representing the commercial financial sector; Lockheed Martin Information Systems & Global Solutions (IS&GS), representing the U. S. defense industrial base; and the United States Postal Inspection Service (USPIS), representing government.

Members benefited by having access to such a diverse set of organizations that represented several of the market sectors to which CERT-RMM applies. This organizational diversity was often cited by members and CERT staff as one of the key benefits of the first RUG Workshop Series.

2.2 Overview of CERT-RMM

CERT-RMM is a capability-focused maturity model for process improvement that reflects best practices from industry and government for managing operational resilience across the domains of

¹ The RDT consists of CERT staff members who support the RUG Workshop Series.

security management, business continuity management, and aspects of information technology (IT) operations management.² CERT-RMM defines operational resilience as

the emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

Through CERT-RMM, these best practices are integrated into a single model that provides an organization with a transformative path from a silo-driven approach for managing operational risk to one that is focused on achieving resilience management goals and supporting the organization's strategic direction [Caralli 2011].

CERT-RMM incorporates many proven concepts and approaches from the SEI's process improvement experience in software and systems engineering, service engineering, and acquisition. Foundational concepts from Capability Maturity Model[®] Integration (CMMI[®]) are integrated into CERT-RMM to elevate operational resilience management to a process approach and provide an evolutionary path for improving capability.³ Practices in the model focus on improving the organization's management of key operational resilience processes. This improvement enables high-value services to meet their mission consistently and with high quality, particularly during times of stress and disruption [Caralli 2011].

CERT-RMM helps to ensure that the organization's important assets—people, information, technology, and facilities—effectively support business activities and services. The model serves as a foundation from which an organization can measure its current competency, set improvement targets, and establish plans and actions to close any identified gaps. As a result, the organization repositions and repurposes its security, business continuity, and IT operations activities and adopts a process improvement mindset that helps to keep services and assets productive in the long term [RUG 2011].

The context for CERT-RMM is shown in Figure 1.

² For more information about CERT-RMM, refer to the book titled *CERT[®] Resilience Management Model: A Maturity Model for Managing Operational Resilience* and the CERT Resilience Management Model pages on the SEI website [Caralli 2011, RMM 2012].

[®] Capability Maturity Model and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

³ For more information about CMMI, refer to the CMMI pages on the SEI website [SEI 2012a].

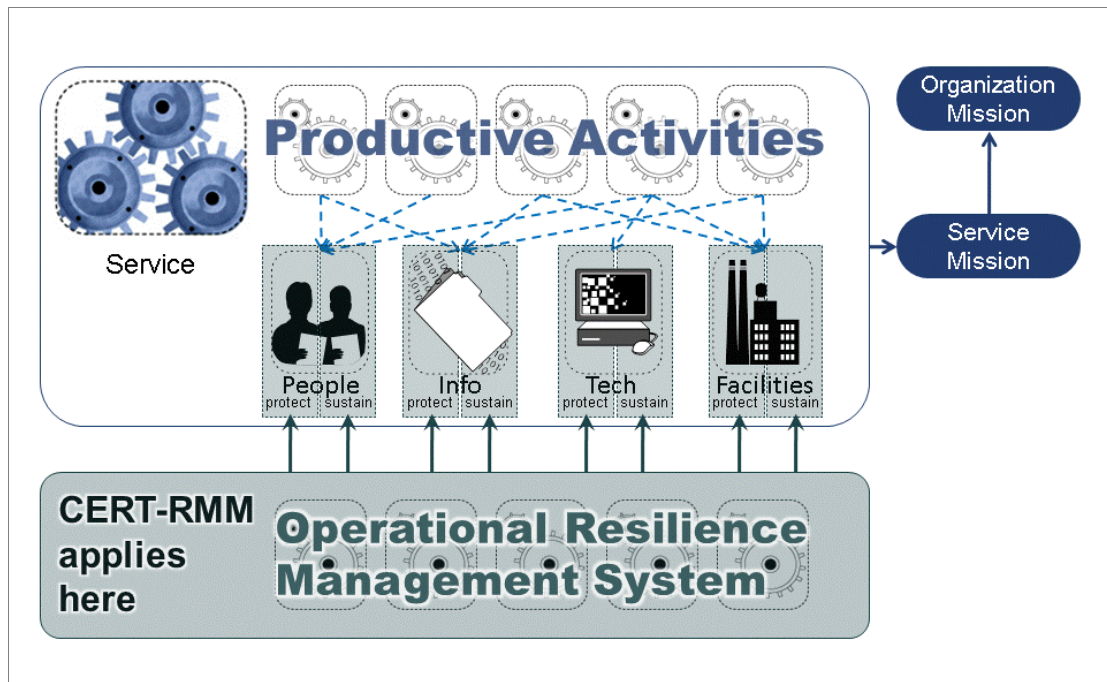


Figure 1: CERT-RMM Context

3 Architecture of the First RUG Workshop Series

3.1 Background

The RDT developed an initial architecture that described the intent of each segment of the first RUG Workshop Series. The architecture provided prospective members with an idea of what was to come and provided RDT staff with a roadmap to follow as the series progressed. The architecture was reviewed by members and updated in advance of each individual workshop.

We summarize the first RUG Workshop Series architecture, as it evolved, in the following sections. The architecture describes advance preparation for the entire workshop series and for each individual workshop, topics to be covered in sequential order, takeaways, outcomes, and expected preparation for each subsequent workshop.

As a result of conducting the first RUG Workshop Series, we developed an improved architecture, which we will use to guide future workshops. We summarize key improvements in Section 8 of this report.

3.2 Advance Preparation

Representatives from all member organizations were interviewed in advance of the first RUG Workshop Series. These interviews occurred from October 2010 to the start of Workshop 2 in May 2011, when the CMU team joined the effort. As part of each member interview, the RDT asked the questions that are listed in Table 1.

Table 1: Preparatory Questions

1. Why are you interested in CERT-RMM?
 - a. Are you actively using CERT-RMM in your organization? If so, how? If not, do you plan to use it?
 - b. Is your use of or interest in CERT-RMM most related to 1) business continuity, 2) security, 3) IT operations, 4) operational risk and resilience management in general, or 5) all of these?
 - c. Are you interested in specific process areas (PAs)? If so, which ones?
2. What are your top three expectations and desired outcomes for the first RUG Workshop Series and for the RUG Workshop Series in general?
3. Are you interested in becoming a CERT-RMM lead appraiser or instructor? If so, in what time frame?
4. We would like to use resilience measurement challenges, objectives, and example measures from participants in discussions and as examples in the workshop series. Would you or your organization be willing to openly share such experiences and examples with other workshop series members?
5. Is there anything else that you would like to share regarding your participation in the CERT-RMM Users Group?

We also required that members

- complete the Introduction to CERT-RMM course
- become familiar with CERT-RMM publications, webinars, podcasts, and the book *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience* [Caralli 2011], which describes CERT-RMM Version 1.1
- prepare a 15-20 minute presentation that addresses the following questions:
 - What are you doing today about resilience?
 - What are your top three to five issues and uncertainties in your current resilience practices?
 - What measures do you use to manage resilience?

The RDT analyzed and synthesized interview data and determined that this particular group of members would be most interested in participating in a workshop that focuses on CERT-RMM model implementation and improvement, which involves leading RUG members through a CERT-RMM-based improvement cycle using member-declared improvement objectives that meet organizational goals.

At this point in the preparatory phase, none of the member organizations were interested in pursuing lead appraiser or instructor certification. Because of this, the RDT did not include this topic in the RUG Workshop Series. We subsequently learned that some members of the CMU and Lockheed Martin (LM) teams did have such interests; therefore, we took follow-up action to remedy this after Workshop 4.

4 Workshop 1: Planning

RUG members from the DFS, LM, the USPIS, and the CERT RDT attended this workshop, which was held March 15-16, 2011 in Pittsburgh, PA. The CMU team did not join this workshop series until Workshop 2.

4.1 Advance Preparation

In preparation for Workshop 1, we asked members to prepare slides that provide a brief introduction of themselves, their organization, their current resilience activities (if any), and the top three to five resilience concerns and issues.

We also asked members to think about improvement objectives that could be implemented in a project lasting 10-12-months. Members came to Workshop 1 prepared to discuss a small number of improvement objectives that they wished to declare and the rationale for each objective. We set expectations with members so they understood that the improvement objectives were to be business oriented and operational in nature, not specific to CERT-RMM.

4.2 Topics

Table 2 lists the topics that we presented and discussed during Workshop 1.

Table 2: Workshop 1 Topics

Workshop 1 Topics

- first RUG Workshop Series initial architecture and plan
- member organization (initially DFS, LM, and the USPIS) presentations including an organizational overview, objectives for the first RUG Workshop Series, and initial improvement-project objectives
- a presentation by LM Enterprise Business Resilience Services that described the company's initial experiences in
 - selecting CERT-RMM as its improvement model of choice
 - conducting CERT-RMM appraisals for improving corporate-wide business continuity, IT disaster recovery, crisis management, and pandemic-planning activities
- a presentation template for gaining senior-management sponsorship
- organizational scoping, applied to each member's improvement objective
- CERT-RMM model scoping, applied to each member's improvement objective
- an overview of the CERT Insider Threat Project⁴
- member feedback about Workshop 1

Prior to the workshop, members had selected candidate improvement objectives based on a range of factors including the following:

- respond more effectively to high-profile, high-impact incidents
- work more effectively with supply chain partners

⁴ For more information about the CERT Insider Threat Project, visit the CERT website (http://www.cert.org/insider_threat).

- satisfy specific compliance requirements more effectively
- integrate aspects of CERT-RMM with current standards and process models
- address directives from senior executives

Throughout this workshop series, we regularly discussed the definition of *operational resilience* (presented in Section 2). We also discussed topics related to deriving specific interpretations of operational resilience for

- information security, business continuity, IT operations, and software/system development
- each member's specific business. We asked ourselves, "What does operational resilience mean to us and our ability to fulfill our mission and meet business objectives?"

Ongoing interpretation and tailoring of the intent of CERT-RMM as applied to each member organization's improvement project occurred throughout the first RUG Workshop Series.

For organizational and model scoping, discussions included fine-grained scoping options based on CERT-RMM processes and practices of interest, the selected organizational unit(s) that will benefit from the improvement, the differences between CERT-RMM and CMMI (for those organizations that have already adopted it), and other caveats. Discussions also included whether the scope should be at the process area (PA) level or the practice level. Members were encouraged to choose their scoping granularity based on their process-improvement objectives. To facilitate this process, the RDT distributed a spreadsheet that could be used for CERT-RMM model scoping. Workshop members spent considerable time honing their respective improvement objectives.

4.3 Outcomes

Takeaways and outcomes from Workshop 1 included the following:

- considerations for refining improvement objectives
- a method for determining CERT-RMM model and organizational scope based on improvement objectives
- a method for diagnosis based on CERT-RMM Compass, a self-administered survey questionnaire
- composition of a CERT-RMM improvement plan and approach based on the SEI IDEALSM method (See Figure 2.)
- a brief description of CERT-RMM licensed roles and the certification process
- confirmation of dates for successive workshops based on
 - a fuller understanding of the work that needs to be conducted between workshops
 - a desire to accelerate improvement-project implementation
 - refinements to the RUG architecture and plan
- beneficial insights from information-sharing sessions and feedback

SM IDEAL is a service mark of Carnegie Mellon University.

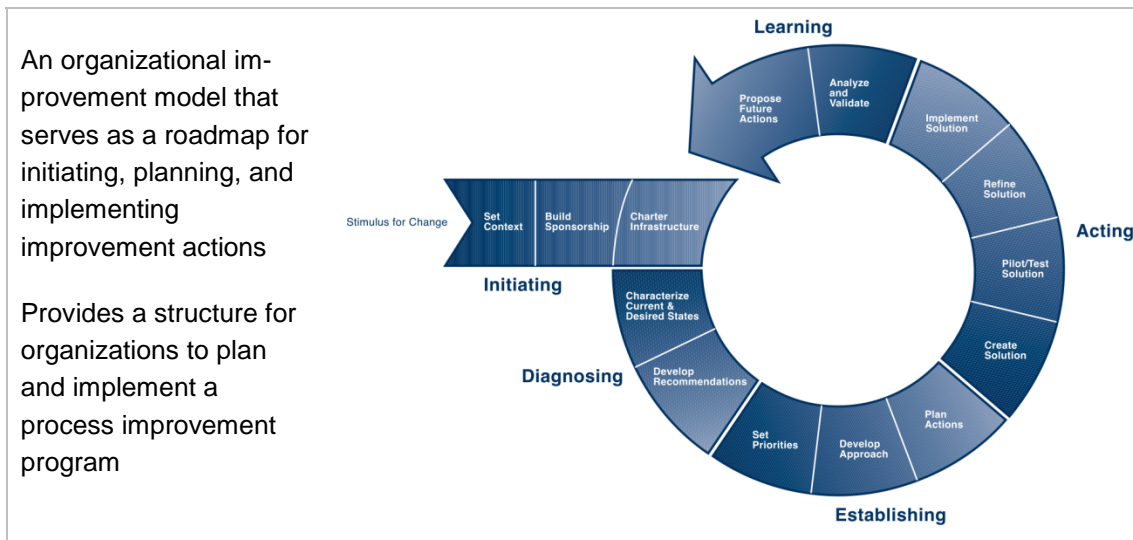


Figure 2: The SEI IDEAL Model [McFeeley 1996]

4.4 Preparation for Workshop 2

In preparation for Workshop 2, members

- defined and refined improvement objective(s), including providing
 - rationale for selection (one or two slides)
 - a list of the objectives that were considered and rejected with rationale
- described the organizational scope (one or two slides, including an illustration of the scope on a member organizational chart)
- depicted the CERT-RMM model scope by process area and practice (We provided an Excel spreadsheet to members.)
- developed a sponsor presentation (i.e., a plan to garner support for the improvement project from the project sponsor)

5 Workshop 2: Improvement Objective

RUG members from the CMU, DFS, LM, and USPIS project teams attended this workshop, which was held May 10-11, 2011 in Pittsburgh, PA. Between Workshops 1 and 2, the RDT decided that the first RUG Workshop Series represented an excellent opportunity to identify a CERT improvement objective and have a CERT team participate in the RUG in the same fashion as the other member teams. Thus the CERT Resilience Enterprise Management (REM) Team also attended and presented at Workshop 2.

5.1 Advance Preparation

In preparation for Workshop 2, members completed the assignments described in Section 4.4 of this report.

5.2 Topics

Table 3 lists the topics that we presented and discussed during Workshop 2.

Table 3: Workshop 2 Topics

Workshop 2 Topics

- member organization (CMU, DFS, LM, USPIS, and CERT REM) presentations including an updated improvement-project objective, organizational scope, model scope, and sponsor presentation
- project-improvement method/lifecycle based on the SEI's IDEAL model, as modified for CERT-RMM⁵ (See Figure 3.)
- organizational and model improvement scope, and whether the intent of the diagnosis is to evaluate an intent to improve (as described in policies and plans) or the actual implementation
- the distinctions between SCAMPI class A, B, and C appraisals and CERT-RMM Compass^{6,7}
- the types of evidence that are collected and reviewed during diagnosis/appraisal, their distinctions (e.g., all policy artifacts, all affirmations, or all implementation artifacts), and the value of using a consistent body of evidence
- various approaches for data collection and diagnosis of the organization's current state based on
 - the improvement objective, organizational scope, and model scope
 - sharing of member experiences
 - the benefit of surveying people as a group to improve the fidelity of answers
 - the opportunity for participants to interact
- the value of having defined processes in place as described in the Organizational Process Definition (OPD) and Organizational Process Focus (OPF) PAs and the value of having a process asset library
- preparation of diagnostic findings for Workshop 3
- team work sessions to apply methods and discussions to their teams' specific projects and identify modifications to improvement objectives, organizational scope, and model scope
- an overview of the CERT research program and future plans
- an overview of the CERT Digital Intelligence and Investigation Directorate (DIID) forensics work⁸
- member feedback about Workshop 2

⁵ One member expressed a preference for using Six Sigma's DMIAC (Design, Measure, Analyze, Improve, Correct) method instead of IDEAL.

⁶ SCAMPI stands for Standard CMMI Appraisal Method for Process Improvement. For more information about SCAMPI, see the 2011 handbook titled *Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A, Version 1.3: Method Definition Document* [SCAMPI 2011].

⁷ A Compass survey is closest to a class C but does not require a plan and does not cover the generic goals (GGs) and GPs.

⁸ For more information about the work of the CERT DIID, visit the CERT website (<http://www.cert.org/forensics/>).

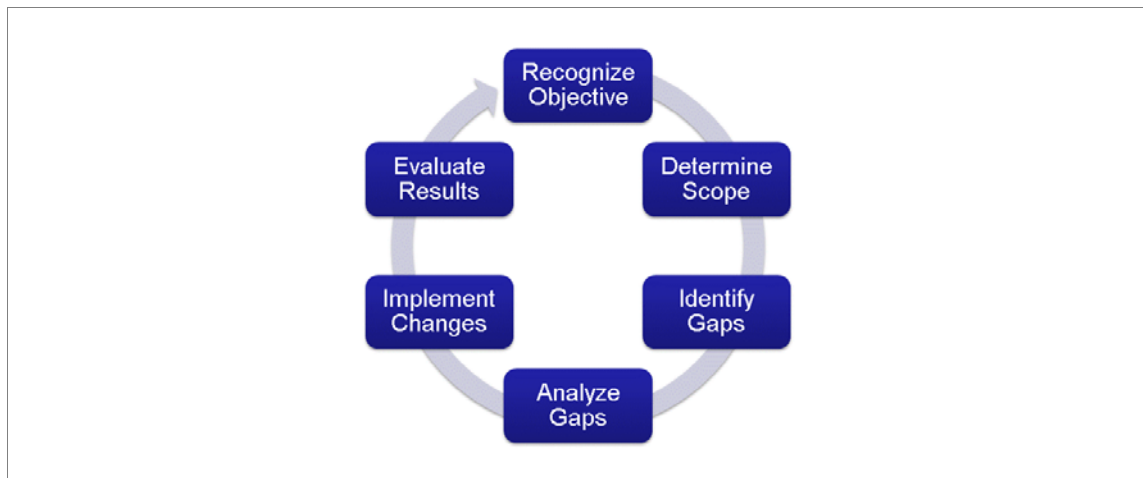


Figure 3: CERT-RMM Improvement-Project Lifecycle

Key discussion points included CERT-RMM variation of the IDEAL model, since this made more sense to RUG members. During Workshop 2, participants started to tease out key characteristics of effective and ineffective organizational scope and model scope. For example, workshop members noted that it is important to ensure that the gaps selected for action resulting from a diagnosis are under the control of the sponsor. This will allow organizations to make forward progress unencumbered. In addition, workshop members noted that when organizations are just getting started, it is important to select a narrow model scope—perhaps just a few specific practices (SPs). (This is an example of the proverb “walk before you run.”)

When performing a diagnosis, it is important to frame diagnostic questions in language that is meaningful to participants. Additionally, one member stated that when performing a diagnosis, it is helpful to have a wide range of objectives beyond the stated improvement objective. It is beneficial to ask questions such as

- Did this approach work?
- How well did it work?
- If the approach did not work, how should we handle similar situations in the future?

5.3 Outcomes

Takeaways and outcomes from Workshop 2 included the following:

- a greater appreciation for the thought and effort required to effectively define organizational scope and model scope so that you can make forward progress in a reasonable period of time
- methods and templates for determining practices and gaps in practice to meet improvement objectives based on the model scope
- refinements to the organizational scope and model scope based on the planned diagnosis
- a CERT-RMM improvement plan and approach based on the IDEAL model, as modified for CERT-RMM (See Figure 3.)
- beneficial insights from information-sharing sessions and feedback

5.4 Preparation for Workshop 3

In preparation for Workshop 3, members

- updated improvement objectives, the organizational scope, and the model scope based on Workshop 2 discussions and the diagnosis of their current state
- provided the results of their diagnosis (by practice, across organizational scope) and submitted the results to the RDT two weeks before Workshop 3. We asked members to include the following information:
 - strengths, opportunities, weaknesses, and gaps (local and systemic)
 - feedback on the use of the diagnostic method of choice (Members used either CERT-RMM Compass or SCAMPI.)
 - activities required to prepare the organizational team to conduct the diagnosis (e.g., awareness, training, ability to participate in the diagnostic process)
 - recommendations about diagnostic activities (e.g., what worked well, what did not work well)
 - prioritized actions resulting from the diagnosis
 - examples of useful artifacts (e.g., processes, checklists, templates, methods, and tools)
- participated in teleconferences between Workshops 2 and 3 to assist with diagnosis, as needed

6 Workshop 3: Diagnosis

RUG members from the CMU, DFS, LM, USPIS, and CERT REM project teams attended this workshop, which was held August 30-31, 2011 in the SEI, Arlington, VA office.

6.1 Advance Preparation

Advance preparation for Workshop 3 consisted of completing the assignments described in Section 5.4 of this report.

6.2 Topics

Table 4 lists the topics that we presented and discussed during Workshop 3.

Table 4: Workshop 3 Topics

Workshop 3 Topics

- member organization (CMU, DFS, LM, USPIS, and CERT REM) presentations including
 - diagnostic results
 - initial gaps for action planning
 - any updates to improvement-project objective, organizational scope, and model scope
 - lessons learned
- member estimates of the effort involved in conducting the diagnosis
- a description of CERT work in process definition and measurement as a key foundation for implementing improved processes and measuring the extent to which they are adding value [Allen 2010, 2011a, & 2011b]
- criteria for determining when to commit resources to define a process
- process and procedure definition templates, with examples
 - one member suggested using lean Six Sigma and other techniques to streamline the process
 - one member shared an alternative process definition template and example [Allen 2011b]
- a measurement template, with examples
- discussion to brainstorm measures of success for the first RUG Workshop Series
- an overview of the work of the CERT Network Situational Awareness Team⁹
- an overview of the CERT work in standards-based, automated remediation¹⁰
- member feedback about Workshop 3

Some of the criteria and success factors that members shared for determining when to commit resources to define a process include the following:

- The process is highly repeatable.
- The process, while performed infrequently, needs to be completed the same way each time it is performed. (It is important that the process is executed consistently by those performing it.)
- It is important to understand the current process before altering it.

⁹ For more information about the work of the CERT Network Situational Awareness Team, visit the CERT website (<http://www.cert.org/netsa/>).

¹⁰ For more information about the Security Content Automation Protocol (SCAP), refer to the NIST SCAP website (<http://scap.nist.gov>).

- Measure process performance for the purpose of improvement.
- There are risks associated with different staff members performing the process differently.
- It is important to meet compliance obligations.
- Capture essential corporate knowledge.
- Clearly communicate to staff members what needs to be done.
- Establish a baseline for measurement.
- Link policy to procedure to process, and help to enforce policies.

Members suggested collecting and analyzing the following measures that characterize RUG performance and success. Several of these measures will be more meaningful when collected over the course of multiple workshop series. (This list is presented in no particular order.)

- number of organizations participating
- number of improvements identified; number of improvements made
- change in member improvement-project objectives (quantity, scope, etc.)
- change in member improvement-project scope (e.g., the number of total organizations participating, number of CERT-RMM PAs, SPs, or GPs [generic practices]). (This measure and the one before it will help set member expectations for future RUGs.)
- ability to accommodate member ingress and egress
- reduction in barriers to becoming a member of the RUG (For example, it would be easier to participate if the RUG offering included the Introduction to RMM course.)
- number of changes/improvements (to the agenda, homework assignments, architecture, etc.) in response to members' suggestions
- closed audit items as a result of RUG improvement projects
- number of members' professional development objectives satisfied
- CERT-RMM certification requirements met and credentials granted
- extent of convergence among CERT-RMM domains represented by RUG member teams (e.g., business continuity/disaster recovery, information security, IT operations)
 - RUG entry criteria—members from a specific organization represent all three CERT-RMM domains
- number of met/unmet members' expectations
- number of members who recommend the RUG Workshop Series to colleagues
- number of members willing to present at future RUG Workshop Series
- extent of continued use of RUG methods (+6 month and +12 month check-in)

6.3 Outcomes

Takeaways and outcomes from Workshop 3 included the following:

- methods and templates for defining processes and process-related measures
- CERT-RMM improvement-project lifecycle in support of action planning
- beneficial insights from information-sharing sessions and feedback

6.4 Preparation for Workshop 4

In preparation for Workshop 4, members

- provided comments/feedback on the RUG member data-handling procedure, data information asset profile, and the Handling Customer Data process as it applies to RUG member data. (These specific examples were provided as part of the process-definition discussion.)
- provided feedback on the use of the Compass survey
- selected at least one activity that required improvement as presented and discussed at Workshop 3
- defined at least one process and one measure, using the templates provided or a variation of them
- began to implement one improved activity, with at least one measure
 - If updating an existing process, the organization is more likely to be able to start collecting measures.
 - If developing a new process, the organization may not have sufficient time to collect measures.
- prepared to report progress (including providing updates to organization scope and model scope)
- collected and reported the effort they expended in performing this preparation work

7 Workshop 4: Improvement Progress

RUG members from the CMU, DFS, LM, USPIS, and CERT REM project teams attended this workshop, which was held January 31 to February 1, 2012 in Tampa, FL. Due to the extended time between Workshops 3 and 4, the RDT scheduled a check-in call with available members on November 30, 2011.

7.1 Advance Preparation

Advance preparation for Workshop 4 consisted of completing the action items and assignments described in Section 6.4 of this report.

7.2 Topics

Table 5 lists the topics that we presented and discussed during Workshop 4.

Table 5: Workshop 4 Topics

Workshop 4 Topics

- member organization (CMU, DFS, LM, USPIS, and CERT REM) presentations describing improvement-project results to date, defined processes, defined measures, lessons learned, effort expended, and post-RUG next steps
- summaries by two member organizations that continue to define, refine, and narrow the model scope to ensure that near-term, measurable results can be produced
- characteristics that may support effective socialization of CERT-RMM within organizations
- difficulties in clearly defining risk tolerance and risk threshold
- new CERT research in analyzing cases of resilience success and failure
- discussion of the relationship of Six Sigma and Supplier, Input, Process, Output, Customers (SIPOC) methods for this type of improvement effort
- member participation in the 2012 Software Engineering Process Group (SEPG) Conference RUG Panel [SEI 2012d]
- plans for future RUG Workshop Series; members noted that the biggest stumbling block to increasing RUG participation is selling the value proposition within their organizations
- an overview of the CERT Smart Grid Maturity Model (SGMM) Project [SEI 2012c]
- an overview of the upcoming CERT research in resilience case analysis
- member feedback on topics to be covered in the RUG Workshop Series report (this document)
- member feedback about Workshop 4 and the first RUG Workshop Series

Characteristics that may support effective socialization of CERT-RMM within organizations include the following:

- Choose an organizational scope and model scope that you can control so that you are able to make forward progress and demonstrate results without having to convince other stakeholders.
- Understand your culture in terms of how best to introduce a new idea.
- Understand the business rhythm to help determine the appropriate ongoing processes and activities to attach this work to. For example, strive to capitalize on a current, hot initiative and demonstrate how to add value.

- Use the terms and language of the organization, not those of CERT-RMM. For example, use the term “proof of concept” instead of “appraisal.” Several members advocated “putting the book in the drawer.” In other words, they advised their peers not to showcase or focus on CERT-RMM; instead, they should start with the organizational problem being addressed and keep the knowledge of the model within the improvement team. Frame assessment questions in terms that are meaningful to those being interviewed; avoid using “model-ese.”
- Build upon diagnostic methods, such as the audit and compliance processes, that are already being used within the organization; add CERT-RMM constructs to these methods.
- Select a specific and narrow topic as you begin to assess your current state. For example, ask yourself
 - How do we escalate incidents?
 - What are the various thresholds for involving specific levels of management?
- When presenting to senior executives, keep in mind their WIIFM (What’s In It For Me?) perspective.

Several RDT members who have participated in CERT-RMM appraisals have indicated that you truly do not understand how to fully apply the model until you conduct an appraisal.

Members discussed additional criteria for investing in process definition, including when the activity involves cross-functional areas or groups and when the activity is related to processes that must be done the same way even if they are done infrequently (examples include generating a VPN¹¹ certificate and configuring a laptop).

CERT-RMM has been used for the following purposes: diagnosis, internal improvement, policy review, intent review, strategic planning, comparison with peers within a given market sector, gap analysis, and independent validation of process improvement efforts not based on CERT-RMM.

Members provided the following feedback on the benefits of participating in the RUG Workshop Series:

- They have a better understanding of CERT-RMM and how to implement it.
- It was valuable to have practical guidance on how to integrate business continuity/disaster recovery concerns with those of information security.
- It was beneficial to work with a knowledgeable, committed support group rather than going it alone.
- Expanding the scope of their improvement projects beyond information security was a worthwhile pursuit.
- It was useful to take a project from beginning to end.
- It was helpful to work on bigger pain points and the highest priority issues.
- It was helpful to have the opportunity to demonstrate success before evangelizing CERT-RMM to others.

¹¹ VPN stands for virtual private network.

- It was helpful to have the opportunity to tackle a problem strategically as contrasted with the more typical, more tactical technology-centered problem.
- It was valuable to 1) have diversity in member organizations and 2) hear their respective views while recognizing that it would also be useful to participate in a sector-specific RUG to address common problems.
- It was valuable to hear about the CERT-RMM product and service lifecycle and how it has been applied—from service and solution development to operations.
- It was beneficial to be part of the beginning of something—to be on the ground floor in starting a new community.
- They
 - appreciated having each workshop serve as a driver for making forward progress on member improvement projects
 - recognized the critical importance of organizational scope and model scope for making forward progress
 - have a better understanding of how to use a descriptive (vs. prescriptive) complex model to pick and choose model content based on the problem of interest
 - have a better understanding of how to present CERT-RMM to the “right” person for sponsorship
- They also appreciated having the opportunity to learn more about other CERT-related work through workshop lunch presentations. (Topics covered during the first RUG Workshop Series included insider threat, CERT research directions, forensics, network situational awareness, security automation and content protocols (SCAP), resilience case analysis research, and the SGMM.)

Most members indicated that they would recommend RUG participation to their colleagues. RUG members should be open minded; have an early adopter mentality; have the ability to interpret, translate, and adopt; and have the ability to tolerate abstraction and a certain amount of “fuzziness.”

Other recommended qualifications include finding someone who is a strong intermediary, facilitator, and integrator and who is comfortable operating in “stealth” mode. (See the comments on page 17 about putting the book in the drawer and presenting the model in terms that are meaningful to the audience.) Members need to be well respected by their co-workers and be able to command organizational attention when they recommend change. It is also useful for members to have experience with organizational change.

In terms of member qualifications, members would not recommend those who require more detailed, prescriptive guidance and those who are advocates of a “by the book” approach to process.

To increase the likelihood of success, the RDT intends to use these characteristics as criteria for evaluating future RUG members.

7.3 Outcomes

Takeaways and outcomes from Workshop 4 included the following:

- confirmation on member progress to date, course correction, and guidance on next steps, from peers and CERT staff
- opportunities to influence the RUG Workshop Series report (this document) by providing feedback
- opportunities to influence future RUG Workshop Series offerings by providing feedback
- opportunities to make member work visible via the SEPG conference panel and the RUG Workshop Series report (this document)
- ability to share and hear beneficial insights through information-sharing sessions and feedback

Following the completion of Workshop 4, all member organizations provided slides in support of the SEPG North America Conference panel titled “Applying CERT-RMM: Users Group Workshop Experiences.” These slides are available in the appendix of this report.

8 Improvements for Future RUG Workshop Series

RUG members contributed numerous suggestions for improving future RUG Workshop Series offerings. One particularly noteworthy suggestion was to develop and use a series of case studies starting with Workshop 1. Cases could demonstrate how CERT-RMM can be used to solve particular problems, such as those pertaining to incident management and control. For example, the RDT could present a structured case of a sample improvement project with a scope of one or two practices. With this approach, members could achieve improvement progress on the sample project by Workshops 2 or 3 and use such a case to better understand what they need to do on their own improvement projects.

Having some solid case studies early in the workshop series would help members understand the challenges associated with scoping; this is a topic that was revisited many times during the workshops. In addition to cases developed by the RDT, member organizations should be invited to lead drill-down discussions in process areas that directly relate to their areas of interest.

To aid in guiding the scope of member improvement projects, the RDT should evaluate the hours spent by each member organization across the entire workshop series. This count should include the time members spent preparing for the workshops.

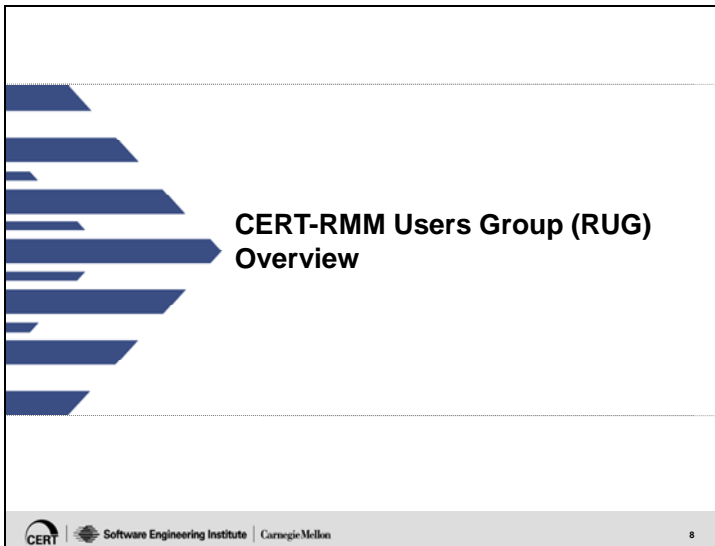
Additional improvement suggestions included the following:

- Provide more robust diagnostic methods, including analysis templates and scoring approaches.
- Establish a working, collaborative workspace infrastructure for sharing RUG workshop artifacts; this would reduce the volume of email and provide a central repository for shared artifacts.
- Set time aside at each workshop to allow members to plan and work on their actions for the next workshop, including setting next steps at the end of Workshop 4.
- Invite lunch speakers, including current and past RUG members, to present on topics of interest in addition to those related to CERT work.
- Consider holding an annual workshop for member organizations that have completed one or more RUG Workshop Series. One possibility would be to hold such an event in concert with SEPG North America so that RUG members can learn from and interact with the CMMI community.

8.1 Contact Us

For further information about the First CERT-RMM Users Group Workshop Series, please contact Dave Ulicne (deu@sei.cmu.edu).

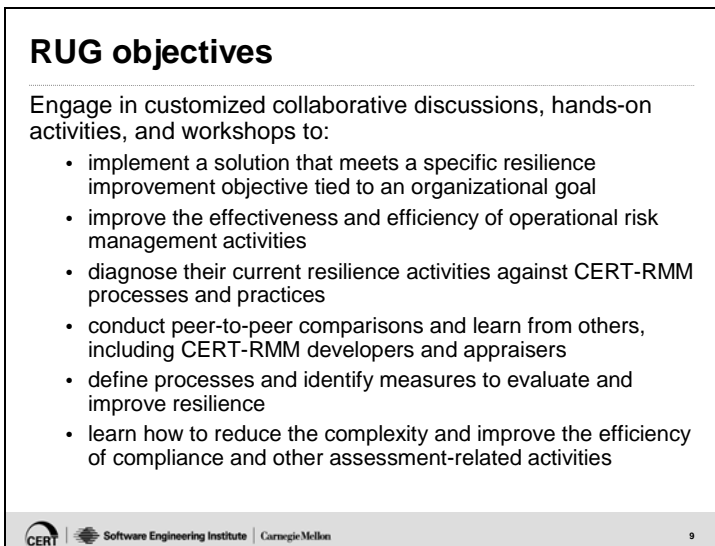
Appendix: 2012 SEPG North America RUG Panel Slides



The slide features a decorative graphic on the left consisting of several horizontal blue bars of varying lengths, some of which are slightly offset to create a sense of depth. To the right of this graphic, the text "CERT-RMM Users Group (RUG) Overview" is displayed in a bold, black, sans-serif font. At the bottom of the slide, there is a footer containing the CERT logo, the text "Software Engineering Institute | Carnegie Mellon", and a small number "8".

**CERT-RMM Users Group (RUG)
Overview**

CERT Software Engineering Institute | Carnegie Mellon 8



The slide has a white background with a thin horizontal line above the title. The title "RUG objectives" is in a bold, black, sans-serif font. Below the title, the text "Engage in customized collaborative discussions, hands-on activities, and workshops to:" is followed by a bulleted list of seven objectives. The footer at the bottom contains the CERT logo, the text "Software Engineering Institute | Carnegie Mellon", and a small number "9".

RUG objectives

Engage in customized collaborative discussions, hands-on activities, and workshops to:

- implement a solution that meets a specific resilience improvement objective tied to an organizational goal
- improve the effectiveness and efficiency of operational risk management activities
- diagnose their current resilience activities against CERT-RMM processes and practices
- conduct peer-to-peer comparisons and learn from others, including CERT-RMM developers and appraisers
- define processes and identify measures to evaluate and improve resilience
- learn how to reduce the complexity and improve the efficiency of compliance and other assessment-related activities

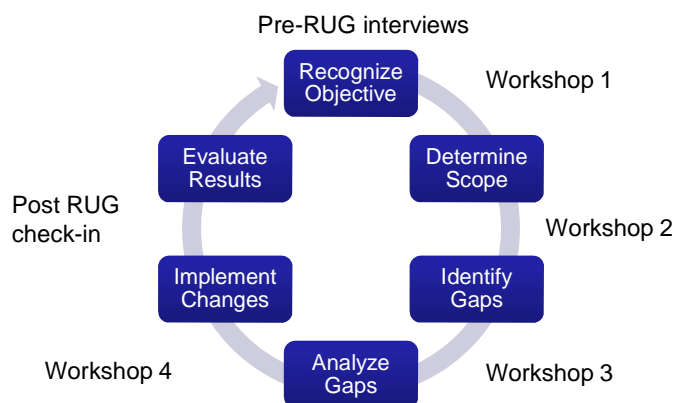
CERT Software Engineering Institute | Carnegie Mellon 9

RUG structure

Four 2-day workshops conducted over 10-12 months;
conference calls in between workshops

Members identify needs and objectives for their
specific workshop series in advance

RUG “Architecture”



Workshop 1: Planning

- initial improvement objective, guidelines for determining organizational scope, and CERT-RMM scope, plans for the workshop series

Workshop 2: Improvement objective

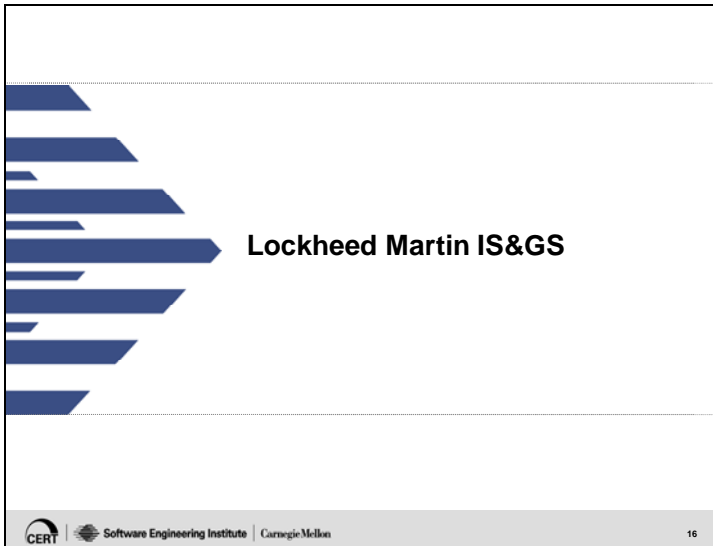
- finalize objective, prepare for diagnosing current state, prepare for improvement

Workshop 3: Diagnosis

- present diagnostic results, evaluate and prioritize gaps, select 1-2 gaps for improvement, prepare for process definition and measurement

Workshop 4: Improvement progress

- report on actions taken, lessons learned, next steps, defined processes, defined measures
- post-RUG 60-day check-in



Lockheed Martin, Information Systems & Global Solutions (IS&GS)

- 30,000 highly skilled professionals bringing together the full range of the corporation's information competencies in information technology solutions, management services, and advanced technology expertise.
- Nearly \$10 billion in sales
- Leading federal services and information technology contractor with a strong heritage of delivering world-class solutions and delivering advanced technology across a broad spectrum of civil and defense domains.

© 2012 Lockheed Martin Corporation. All rights reserved.

17

Strategic Process Engineering

- Reporting to CTO

- Analyzes current and future IS&GS business directions to identify and deploy the management and engineering processes needed to enable affordable performance on programs and address our rapidly evolving customer environment.
- Assists product lines with understanding and benchmarking program performance through process analytics and Lean/Six Sigma activities to ensure Performance Excellence.
- Provides ISO Standards Leadership, CMMI consultation and benchmarking, ITIL consultation, Agile technical support, and Services analysis and benchmarking.

© 2012 Lockheed Martin Corporation. All rights reserved.

18

CERT® Resilience Management Model

- Great fit for LMCO and IS&GS business
 - Internally and for our customers
- Great fit for current IS&GS needs
 - Cyber Security, Cloud Computing
- Great fit for charter of Strategic Process Engineering
 - Identify and deploy processes to support our programs
 - Benchmark our programs to determine current gaps
 - Complements current work in CMMI® and ISO 27001

© 2012 Lockheed Martin Corporation. All rights reserved.

19

CERT® RMM Users Group

- Helped us understand current usage of model constructs
- Helped us understand current issues companies face in resilience management
- Provided different perspectives on the various process areas
 - So that we more fully understood intent
- Allowed us to get involved in the interchange of ideas surrounding resilience

© 2012 Lockheed Martin Corporation. All rights reserved.

20

Example

- As CMMI practitioners, we thought we had a thorough understanding of Risk Management
 - CERT-RMM Users Group helped us understand that more is required for resilience
 - Organizational strategy – enterprise wide initiative
 - Concept of “acceptable risk”
 - Risk tolerances and appetite for organization
 - Extended risk sources and categories – focused on operational risk

© 2012 Lockheed Martin Corporation. All rights reserved.

21

How We Used the Model

- Introduced CERT-RMM-focused questions into our CMMI-DEV SCAMPI B Interviews
 - Risk Management
 - Resilience Requirements Development
 - Resilience Requirements Management
 - Resilient Technical Solution Engineering
 - External Dependencies Management
- Goal was two-fold:
 - Were there resilience gaps on our programs?
 - Could we incorporate elements of this model into our SCAMPI Bs?

© 2012 Lockheed Martin Corporation. All rights reserved.

22

Results

- Added questions to 8 SCAMPI Bs across two product lines
- Were there resilience gaps on our programs?
 - No obvious ones, although there were areas that could be improved
- Could we incorporate elements of this model into our SCAMPI Bs?
 - Quite easily, even for those B/C Team Leads that didn't have training in CERT-RMM

© 2012 Lockheed Martin Corporation. All rights reserved.

23

US Postal Inspection Service



CERT-RMM Users Group

Revenue & Product Security

UNITED STATES
POSTAL INSPECTION SERVICE
11/04/2010 | 1



Organization

- U.S. Postal Inspection Service (USPIS) - one of two law enforcement arms of the US Postal Service (USPS).
- USPS-Office of Inspector General - responsible for all internal crimes within the USPS.
- USPIS - responsible for protecting the security of the USPS brand name, facilities, information and technical assets.
- USPIS enforces over 200 federal statutes - electronic crimes, mail fraud, mail theft, identity theft, child exploitation and prohibited mailings such as bombs, biological and chemical threats.
- USPIS Revenue & Product Security group (members of the CERT-RMM Users Group) specifically investigates external computer security incidents targeted at USPS and its customers and makes recommendations to USPS-IT for information security improvements.
- USPS-IT has ultimate decision to accept or reject recommendations.



How USPIS used CERT-RMM

- CERT-RMM assisted USPIS to improve processes within computer incident response and management.
- Enhanced communication with relevant internal stakeholders and assisted in defining and enhancing incident response, specifically:
 - Identification
 - Containment
 - Eradication
 - Recovery
- USPIS recommended additional policies added to existing USPS-IT security policies to incorporate law enforcement functions.
- USPIS created and recommended use of a more profound computer incident handling guide similar to NIST and CERT to improve effectiveness of response to a computer-related incident.

Revenue Fraud & Product Security

UNITED STATES
POSTAL INSPECTION SERVICE
11/04/2010 | 3




Value of CERT-RMM

- Network with other academia, private, and governmental organizations.
- Immediate access to knowledgeable CERT-RMM instructors who provided valuable feedback to project improvement.
- Access to various types of documents and templates to assist with narrowing project scope, processes, and procedures.



Revenue Fraud & Product Security

UNITED STATES
POSTAL INSPECTION SERVICE
11/04/2010 | 4





Carnegie Mellon University Information Security Office

 Software Engineering Institute | Carnegie Mellon

28

Carnegie Mellon University





- Est 1967 in Pittsburgh, PA
- Global, private research university
- Ranked 22nd
- 15,000 faculty, staff, students
 - 4,000 faculty and staff
 - 11,000 students
 - 84,000 alumni
- Entrepreneurial, highly distributed, 'scrappy'

Information Security Office
www.cmu.edu/iso

29

Our RMM Journey

Carnegie Mellon

"I'd been searching for tools and techniques to conduct security risk assessments and to evaluate and improve the capability of our information security program. While pursuing the first, via OCTAVE Allegro training, I became aware of CERT-RMM.



The notion of "resilience" better characterized what our information security program is really about. Further, I saw it as a potential unifying theme for my partners in DR/BC and operations. It explained how our areas of focus interplay to deliver business value.

We exercised the model first within our own incident response function and realized immediate value. The next step was to test it on a more complex improvement goal that crossed process areas. Participation in the RUG facilitated this exercise, showed us the gaps in original thinking, and kept us on track."

Mary Ann Blair

Director of Information Security

Information Security Office
www.cmu.edu/iso

- Apr 2010 – OCTAVE Allegro training
- Oct 2010 – Intro to RMM training
- Nov 2010 – Pilot discussions begin
- Jan 2011 – Compass assessment of Incident Management and Control (IMC) process area begins
- April 2011 - Compass results guide IMC improvement definition
- Apr 2011- RUG invite accepted
- June 2011- February 2012 - RUG participation guides complex, inter-process area improvement effort

30

RUG value proposition

Carnegie Mellon

1. Access to the CERT-RMM experts and discussion amongst members greatly improved our objective scope and understanding of the model.
2. Reviewing and tracking others' progress allowed us to apply and test our model understanding on several other use cases. This gave us lots of additional practice without lots of extra effort.
3. We expanded our professional network beyond our usual types of contacts. This made not only the RUG sessions a more interesting experience but gave us a richer set of professional contacts to share with in the future.
4. The trust we established, and frankly required, allowed us to dig deep into a wide set of issues that can help a project succeed or lead a project to failure. The detours we took were as valuable as the set agenda.
5. Contributing directly to the improvement of the model and supporting materials was a personally rewarding by product of RUG participation.

Information Security Office
www.cmu.edu/iso

31



REM overview

CERT Resilience Enterprise Management team
responsible for CERT-RMM:

- development and transition
- training
- appraisals
- users group
- licensing and certification
- application and tailoring of the model for customer engagements

Use of CERT-RMM

Improvement objective: Protect and sustain customer data in accordance with customer requirements (collect, develop, serve as custodian for)

Model scope: ADM, KIM, RRD

Results to date

- Customer data handling process definition
- Specific customer data procedure definitions
- Information asset profiles
- Defined measures
- Process asset repository
- Stakeholder buy-in



Software Engineering Institute | Carnegie Mellon

34

Value of the RUG

Formalized and documented a key operational process

Better understanding of all aspects of a CERT-RMM process improvement project

Incentivized to develop example artifacts in advance, to assist RUG members with their projects

Developed effort estimates for each improvement project phase

Obtained valuable improvement suggestions for subsequent RUG workshops (case studies, more prescriptive guidance early on)



Software Engineering Institute | Carnegie Mellon

35

Resources

[Caralli 2010] Caralli, Richard A.; Allen, Julia H.; White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2010.

CERT-RMM Users Group Workshop Series:

<http://www.sei.cmu.edu/training/P92.cfm>

CERT-RMM website: <http://www.cert.org/resilience/rmm.html>

CERT-RMM Measurement & Analysis website:

<http://www.cert.org/resilience/rma.html>

CERT Podcast Series: Security for Business Leaders,
specifically podcasts on risk management & resilience:

<http://www.cert.org/podcast/>



Software Engineering Institute | Carnegie Mellon

37

References

[Allen 2010]

Allen, Julia & Davis, Noopur. *Measuring Operational Resilience Using the CERT Resilience Management Model* (CMU/SEI-2010-TN-030). Software Engineering Institute, Carnegie Mellon University, 2010. <http://www.sei.cmu.edu/library/abstracts/reports/10tn030.cfm>

[Allen 2011a]

Allen, Julia & Curtis, Pamela. *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Software Engineering Institute, Carnegie Mellon University, 2011. <http://www.sei.cmu.edu/library/abstracts/reports/11tr019.cfm>

[Allen 2011b]

Allen, Julia; Curtis, Pamela; & Gates, Linda. *Using Defined Processes as a Context for Resilience Measures* (CMU/SEI-2011-TN-029). Software Engineering Institute, Carnegie Mellon University, 2011. <http://www.sei.cmu.edu/library/abstracts/reports/11tn029.cfm>

[Caralli 2011]

Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011. <http://www.sei.cmu.edu/library/abstracts/books/9780321712431.cfm>

[McFeeley 1996]

McFeeley, Bob. *IDEAL: A User's Guide for Software Process Improvement* (CMU/SEI-96-HB-001). Software Engineering Institute, Carnegie Mellon University, 1996. <http://www.sei.cmu.edu/library/abstracts/reports/96hb001.cfm>

[RUG 2011]

RMM Users Group. "CERT Resilience Management Model (CERT-RMM) Users Group Workshop Series." Software Engineering Institute, Carnegie Mellon University, 2011. <http://www.sei.cmu.edu/training/p92.cfm>

[SCAMPI 2011]

SCAMPI Upgrade Team. *Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A, Version 1.3: Method Definition Document* (CMU/SEI-2011-HB-001). Software Engineering Institute, Carnegie Mellon University, 2011. <http://www.sei.cmu.edu/library/abstracts/reports/11hb001.cfm>

[SEI 2012a]

Software Engineering Institute. *Capability Maturity Model Integration (CMMI)*. Software Engineering Institute, Carnegie Mellon University, 2012. <http://www.sei.cmu.edu/cmmi/>

[SEI 2012b]

Software Engineering Institute. *CERT Resilience Management Model*. CERT Program, Software Engineering Institute, Carnegie Mellon University, 2012. <http://www.cert.org/resilience/rmm.html>

[SEI 2012c]

Software Engineering Institute. Smart Grid Maturity Model. Software Engineering Institute, Carnegie Mellon University, 2012. <http://www.sei.cmu.edu/smartgrid/>

[SEI 2012d]

Software Engineering Institute. Software Engineering Process Group (SEPG). SEPG North America. Albuquerque, New Mexico, March 12-15, 2012.
<http://www.sei.cmu.edu/sepg/na/2012/index.cfm>

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE April 2012		3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE Report from the First CERT-RMM Users Group Workshop Series			5. FUNDING NUMBERS FA8721-05-C-0003	
6. AUTHOR(S) Julia H. Allen & Lisa Young				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213			8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2012-TN-008	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12B DISTRIBUTION CODE	
13. ABSTRACT (MAXIMUM 200 WORDS) This report describes the first CERT® Resilience Management Model (RMM) Users Group (RUG) Workshop Series and relays the experiences of participating members and CERT staff. This workshop series comprised four workshops, which took place between March 2011 and February 2012. In this report, we provide a brief overview of the CERT Resilience Management Model (CERT-RMM), describe the architecture for this series of workshops, and present suggestions for improving future RUG Workshop Series.				
14. SUBJECT TERMS CERT Resilience Management Model, CERT-RMM, RUG Workshop, maturity model, process improvement, workshop series			15. NUMBER OF PAGES 48	
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	